PAT-NO: JP410149396A

DOCUMENT-IDENTIFIER: JP 10149396 A

TITLE: COMMERCIAL TRANSACTION SYSTEM

PUBN-DATE: June 2, 1998

INVENTOR-INFORMATION:
NAME
SATO, TETSURO
KITANO, HIROYUKI

ASSIGNEE-INFORMATION:
NAME COUNTRY
ADVANCE CO LTD N/A

APPL-NO: JP08322177

APPL-DATE: November 19, 1996

INT-CL (IPC): G06F017/60, G09C001/00 , H04L009/08

ABSTRACT:

PROBLEM TO BE SOLVED: To rationally and safely perform a commercial transaction by using a virtual card on the communication line of internet or the like and performing communication after converting processing such as enciphering is temporarily executed to card information.

SOLUTION: In the case of registration from a user 12 to a certificate agency CA 13 and a card company PG 14, first of all, the user 12 generates a disclosure key and a cryptographic key, registers this disclosure key to the CA 13 and gets the certificate of that disclosure key. Besides, when the user 12

applies the registration to the PG 14 together with the disclosure key, the PG
14 confirms whether the disclosure key of user 12 is registered in the CA 13 or
not. Then, the CA 13 issues the certificate of the disclosure key registered
by the user 12 to the PG 14. Similarly to a credit card, the PG 14
investigates identity and in the case of OK, the PG 14 sends a credit card
number to the user 12. Thus, the transaction is simplified in comparison with
a conventional commercial transaction using credit cards and without requiring
any special equipment, the commercial transaction is easily performed.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－149396

(43)公開日　平成10年(1998)６月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ａ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｂ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｄ

審査請求　未請求　請求項の数３　ＦＤ　（全 10 頁）

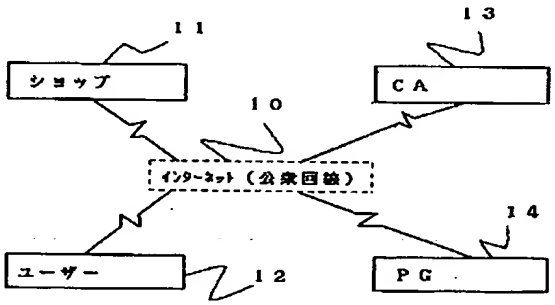
(21)出願番号　特願平8－322177

(22)出願日　平成８年(1996)11月19日

(71)出願人　000126757
株式会社アドバンス
東京都中央区日本橋小舟町５番７号
(72)発明者　佐藤　哲朗
東京都多摩市鶴牧５－37－５－406
(72)発明者　北野　博之
東京都調布市八雲台１－26－５－204

(54)【発明の名称】　商取引システム

(57)【要約】
【目的】従来のクレジットカードを用いた商取引に比べ、それ以上に簡単で、特殊な機器を要せず簡便な商取引を実現する。
【構成】特定の情報により認証可能な状態で連携され、情報を他の形式に変換する手段乃至復元変換する復元手段を有するエンテイテイ；前記変換手段、復元変換手段において情報を変換する為に必要な変換用情報を前記エンテイテイに対し管理するように取り扱うセンタ；よりなり、取引エンテイテイは、前記変換手段に基づいて前記特定の情報を変換情報として出力し、取引認証エンテイテイは、前記変換手段、伝達された変換情報を復元用変換手段により復元された特定の符号に基づいて取引情報を出力することにより、互いの連携を認証可能な符号であって、伝達時暗号化、復号化されることで取り扱われる特定符号で商取引を行う。



1

【特許請求の範囲】
【請求項1】特定の情報により認証可能な状態で連携され、情報を復元可能な状態に変換する変換手段を有するエンテイテイ、
前記変換手段により情報を変換する為に必要な変換用情報を取り扱うセンタよりなり、
取引エンテイテイは、前記変換手段に基づいて前記特定の情報を変換情報として出力し、
取引認証エンテイテイは、変換情報から復元された特定の符号に基づいて取引情報を出力することを特徴とする商取引システム。
【請求項2】前記変換用情報は、自分の秘密鍵によって作成され、前記復号的な変換処理は、相手の公開鍵によりおこなわれる請求項1に記載の商取引システム。
【請求項3】前記変換用情報は、自らに半固定的で且つ公開された識別子に基づいてセンタで作成され、実行時、相手の識別子の入力により、相手と共有する共有鍵を出力することを特徴とする請求項1に記載の商取引システム。
【発明の詳細な説明】
【0001】
【産業上の利用分野】本発明は、電子商取引を行うシステムに関する。
【0002】
【従来の技術】クレジットカードは、本人を認証するに相当する能力を有し、これを正当な所有者が所有する限りに於いては、現金を要しなくても、物品の購入、サービスの提供を受ける事ができる等、利便性を有するものであった。しかしながら、この様に正当な利用者が所有していれば、優れた利便性はあるものの、今現在クレジットカードを取り巻く環境では 盗難、紛失、偽造などの不正使用が売り上げの数%を占めている状態に至っているのが現状であり、署名で本人確認を行っているが、不正使用は防げてない。 更に、クレジットカードにおいては、これに記憶されたデータを読み出す為の機器が必要であり、又その機器使用方法に基づいた手続きも必要であった。また最近のInternetの普及により、オンライン上でクレジットカードによる電子決済の必要性が出てきた。この普及は、家庭等の一般消費者に及ぶものであることから、その取扱いも特定の知識、特殊な専用機器を必要とせずに行われることが希求されるものであった。今現在ではオンライン上では本人確認の方法がないので、FAXでのクレジット番号の送信、電話による本人確認するなどオフライン処理で決済が行われており、通信回線の有効な利用が図られているとはいい難いものであった。
【0003】
【課題を解決するための手段】上記に鑑み本発明は、特定の情報により認証可能な状態で連携され、情報を他の形式に変換する変換手段乃至復元変換する復元変換手段

2

を有するエンテイテイ、前記変換手段、復元変換手段において情報を変換する為に必要な変換用情報を前記エンテイテイに対し管理するように取り扱うセンタよりなり、取引エンテイテイは、前記変換手段に基づいて前記特定の情報を変換情報として出力し、取引認証エンテイテイは、伝達された変換情報を復元用変換手段により復元された特定の符号に基づいて取引情報を出力することにより、互いの連携を認証可能な符号であって、伝達時暗号化、復号化されることで取り扱われる特定符号、すなはち仮想的に設定されたクレジットカードを使用して商取引を行うことで、従来のクレジットカードを用いた商取引に比べ、それ以上に簡単で、特殊な機器を要せず簡便な商取引を実現するものである。本発明は更に以下のようなことも実現する。・暗号を使うことによりカード会社等が直接本人認証を行うことができ、・カード番号のみでカードは実体がないので、実際の店では上記のような問題は起きない。と簡単でスピーディで安全にInternet等の通信回線上でクレジット決済ができるようになり、リスクが下げられ、安全にかつ安い利用料金でクレジットカードを利用できるようになる、というものである。
【0004】本発明で示す特定の情報とは、従来のクレジットカードに記憶または付されている数字、データ、符号その他の情報及びそれらの組合せを示すものであり、重要者は、予めまたは商取引の際、あるいは場合によっては商取引の後（例えば商取引時は仮の符号を使用する場合）、所有していればよいものである。この際の所有とは、ＦＤ，ＭＯ，ＣＤ－Ｒ、ＣＤ、ＩＣカード、ＨＤ、その他汎用性、専用性を有する記憶媒体に記録した形式、あるいは、電子メールを提供するプロバイダ等のサービス業者が提供する記録空間に記録する形式等が例示されるが、特に暗記できる程度のものであれば憶えておくか、手帳等に付したものであってもよい。連携とは、需要者、供給者が、認証管理体が設定する取り決め、システムに同意あるいは付属、参加したことで容認可能な関係または需要者、供給者が、認証管理体が、第三者または機関が設定する取り決め、システムに一時的にまたは持続的に同意あるいは付属、参加、加入したことで、容認可能な関係等を示すもので、事前にまたは取引の後またはその時に連携は発生するものである。本発明で示すエンテイテイとは、人、装置、及びソフトウエア、それらの集合であって、取引に関係を有するもの等を示し、大きく分けて需要、供給、認証管理にわけることができるが、これを分説する。尚、取引形態に応じてその他の区別、分類等も有り得るものであり、特に限定するものではない。本発明で示す需要のエンテイテイとは、一般消費者、クライアント及び取引を行う手段、その他、供給体に対し目的（例えば商品の購入、サービスの提供等）を達成するための手段を有する機関、集合物等を示す。供給のエンテイテイとは、需要のエンテイテ

イが、欲する目的を得ることが可能か、可能と思われるものであって通信媒体上で取引を行う手段を有する販売店、量販店、カタログショッピング業が例示されるが、その他個人及び取引を行う手段、機関、集合物、その他エンテイテイ等を示してもよい。認証管理のエンテイテイとは、取引によって生じる需要と供給間の債権債務を代行したりして、需要、供給と債権債務関係を発生させるものであり、クレジット会社、信販会社、銀行、その他金融機関等の１つまたは複合体及び取引を行う手段の組合せであり、その他、金融取引可能な個人、機関、システム、端末等を示すものである。

【０００５】センタとは、エンテイテイが情報交換を行う際行われる情報の暗号化、復号化の他様式への変換を行う為のその手段の提供、あるいは、各体を認証するデータ、情報を保管し、認証を必要とする際、照合し、その旨を連絡する、或いは関連データ、情報等の自主的又は申請等により、変更、更新、抹消、訂正、修正、削除等の管理するように取り扱うような動作を行うセンター、各種機関、システム、個人等である。尚、これらのエンテイテイ、センタは、例えば、認証管理のエンテイテイがセンタとなる場合等それぞれになる場合や、認証管理のエンテイテイがセンタを兼ねる場合や、それぞれのエンテイテイの一部が合体する場合もある。　　本発明で示す情報伝達の際の情報変換手段としては、主に暗号化手段が用いられる。暗号化方式としては、共有鍵方式、公開鍵方式等が好適にもちいられるが、これに限られるものではない。本発明は、カード番号等の一般にクレジットカード等に記録されている情報のみ使用し、実物は特に必要としないものであると共に、使用時には署名をする代わりに暗号技術を使った本人認証を行うことも可能である。

【０００６】

【実施例】

実施例１

図１に一実施例を利用するための環境の一例を示す。具体的には認証機関CA(Certification Authority)、クレジット管理機関PG(Payment Gateway)等に登録された暗号用の鍵(公開鍵方式やKPS方式等)と暗号アルゴリズム(DES（Data Encryption Standard）、FEAL（清水、宮口、太田：”高速データ暗号アルゴリズムＦＥＡＬ”、電子通信学会技術報告、（情報論）、VOL.80,No.113,IT 86-33,PP.1-6,(1986年））、スクランブル方式、ストリームサイファー等)を使い、メッセージ認証やディジタル署名等で本人認証を行う。 本人認証が済んだら商品名、支払い金額、カード番号等必要な情報を暗号通信でやりとりする。（１０）は、通信回線であり、インターネット、ローカルネット等を示すものであるが、少なくとも、各構成と一方向または他方向の通信が行えるものであれば、通信媒体（光、電波、赤外線等）を問わず、いかなるものであってもよい。（１１）は、ショップ

（販売部）であり、商品、サービスを供給する店舗、量販店、等であり、通信回線を使用して注文を受け、商品等を発送するものである。ショップ（１１）は、通信回線と接続する為の端末、例えば汎用または専用コンピュータ、専用または汎用端末を備えている。本実施例では、通信回線上インターネットを介して通信することを例示していることから、接続利用するに必要な、ダイヤラー、ブラウザ等のソフトウエアを実行可能とする設備を有するものとした。（１２）は、ユーザーであり、ショップ（１１）の商品を購入、サービスの提供を受けるための個人、法人等であり、ショップ（１１）と同様通信回線と接続、通信回線を使用してデータの送受信、データの処理等を行う設備を有する。（１３）は、認証機関（ＣＡ）であり、公開鍵の登録保管、認証等を行う為の有人の機関乃至コンピュータ管理等による無人の機関である。（１４）は、クレジット管理機構（ＰＧ）（クレジット機関部、カード会社と示す場合もある。）であり、クレジットシステムを運営している会社法人、団体、個人等である。クレジット管理機構（１４）もショップ（１１）と同様、通信回線と接続、通信回線を使用してデータの送受信、データの処理等を行う設備を有する。クライアント（ユーザー（１２））、shop（１１）、CA（１３）、PG（１４）はすべてInternet上（１０）に存在し、CA（１３）とPG（１４）は同じ機関であってもよい。複数のクレジット会社が存在する場合は、ひとつの鍵を複数のカード会社で共有してもいいし、カード会社毎に異なる鍵を作ってもよい。

【０００７】暗号方式として公開鍵を用いた場合の本発明の実施例について図２、図３を参照して説明する。公開鍵方式とは、暗号化の鍵と復号化の鍵が別で、片方を公開して公開鍵とし、もう片方を秘密裏に所持して秘密鍵とする方式であって米国特許４２１８５２号、４４０５８２９号公報、特開昭５４－８８７０３号公報等に示される方式が好適に利用されるがこれに限るものではない。図２における各構成は、図１の説明で示したものと同一であり、その説明は省略し、動作の説明をする

【０００８】ユーザー（１２）が認証機関ＣＡ（１３）、カード会社ＰＧ（１４）に登録する際のシステムの動作について説明する。尚、下述の①～⑥と図２の①～⑥はその動作説明上一致するものである。尚、情報の伝達は、全てが通信回線（１０）上で行われるものではなく、その１部又は場合によっては全部において他の手段（郵送、宅配、等）で行われる場合もある。

① ユーザー（１２）は公開鍵と秘密鍵を生成し、認証機関CA（１３）へこの公開鍵を登録する。

② ユーザー（１２）は認証機関CA（１３）から自分が作った公開鍵の証明書をもらう。

③ ユーザー（１２）は公開鍵と一緒にカード会社PG（クレジット管理機構（１４））へ申し込む。

④ カード会社PG（１４）は認証機関CA（１３）へユー

5

ザー（１２）の公開鍵が登録されているかを確認する。

⑤　認証機関CA（１３）はカード会社（１４）に対してユーザー（１２）が登録した公開鍵の証明書を発行する。

⑥　クレジットカードと同様にカード会社PG（１４）が本人調査を行い、ＯＫであればカード会社PG（１４）はユーザー（１２）へクレジットカード番号VCCを送る。

【０００９】次に実際の取引の際の実施例の動作の一例について図３を参照して詳細に説明する。11A,12A,14Aは、秘密鍵実行手段であり、秘密鍵を具備し、対応する入力端11F,12F,14Fより入力されるデータをこの秘密暗号鍵に基づき暗号化し出力するものである。11B,12B,14Bは、公開鍵実行手段であり、対応する入力端11D,12D,14Dから入力される公開鍵に基づき入力される暗号化データを復号化して出力端11E,12E,14Eに出力する。出力端11E,12E,14Eは、復号化データを表示、或は認証の正当性の為の処理をした後、その結果を出力する為のデイスプレイ、ＣＰＵに直接又は間接的に接続される。11C,12C,14Cは、端末入出力手段であり、通信回線、または通信媒体との接続の為の変調、復調手段等のインターフェイスを示すものである。

【００１０】次に取引時の実施例の動作を説明する。この場合、ショップ（１１）、クレジット管理機関（１４）は既に特定、認証されているものとした上で、クレジット番号等のクレジットデータによる商取引について説明する。ユーザー（１２）において、クレジットデータを秘密鍵実行手段（12A）の入力端（12F）に入力する。秘密鍵実行手段（12A）は、秘密鍵を用いてクレジットデータを暗号化し、端末入出力手段（12C）に出力する。端末入出力手段（12C）は、この暗号化データに変調などを施し、ショップ（１２）へ送信する。ショップ（１１）は、端末入出力手段（11C）でこの暗号化データを受信復調し、公開鍵実行手段（11B）へ出力する。公開鍵実行手段（11B）は、入力端（11D）からユーザー（１２）の公開鍵を入力し、この公開鍵に基づいて暗号化データを復号変換して出力端（11E）にユーザー（１２）のクレジットデータを出力する。このクレジットデータにより、ショップ（１１）は、クレジット使用可能かどうかを判別し、判別に疑問がある場合や判別を行わない場合、ショップ（１１）は、このクレジットデータを入力端（11F）へ入力し、秘密鍵実行手段（11A）で秘密鍵により暗号化して、端末入出力手段（11C）に出力する。端末入出力手段（11C）は、このデータを変調して通信回線（１０）上に出力し、クレジット管理機関（１４）に送信する。判別した場合は、その結果を直接ユーザ（１２）に送信する場合もある。クレジット管理機関（１４）は、この暗号化データを端末入出力手段（14C）で復調した後、公開鍵実行手段（14B）へ出力する。公開鍵実行手段（14B）は、入力端（14D）から入力されたショップ（１１）の公開鍵により、暗号化データを復号化し、登録データ処理手段（14G）へ出力する。登録データ処理手段（14G）は、入力されたクレジットデータと、記録されているユーザーデータとの照合を行い、その結果、例えば記録の有無、或いはブラックリスト属否の有無、利用限度額などのユーザー情報を出力端（14E）に出力すると共に、入力端（14F）へ入力する。このユーザー情報は、秘密鍵実行手段（14A）で、秘密鍵により暗号化され、端末入出力手段（14C）、通信回線（１０）を介してショップ（１１）へ伝送される。ショップ（１１）は、この暗号化ユーザー情報を端末入出力手段（11C）を介して、公開鍵実行手段（11B）で受信し、公開鍵実行手段（11B）では、入力端（11D）より、クレジット管理機関（１４）の公開鍵に基づきこの暗号化ユーザー情報を復号化し、出力端（11E）より出力する。この出力されたユーザー情報に基づき、商品購入又はサービスの提供が正当なものか判断し、正当であれば、ユーザー（１２）に商品の配送又はサービスの提供を行う。正当な取引の可否をユーザー（１２）に告げる場合、可否を示す情報を入力端（11F）に入力する。秘密鍵実行手段（11A）は、秘密鍵に基づいてこの可否情報を暗号化し、端末入出力手段（11C）、通信回線（１０）を介してユーザー（１２）へ出力する。ユーザー（１２）は、この可否情報を端末入出力手段（12C）を介して公開鍵実行手段（12B）へ伝達し、更に入力端（12D）にショップ（１１）の公開鍵を入力することで復号化して可否情報を出力端（12E）から出力する。

【００１１】これら各手段は、専用回路或いは目的を達成することが可能な汎用性の回路或は、プログラム化したもの等が示されるが、商取引が汎用性の高い分野で行われることから、特殊な機器を要せず、汎用コンピュータ及びその周辺機器の組み合わせにおけるプログラムの形式で取り扱われることが好ましいものである。尚、秘密鍵等は、それが秘密に保持される必要性があることからＩＣカード、磁気カード、光磁気カード等で示される担体の様なタンパー性を考慮した機器に保存される場合もある。この場合は、この担体を読みだし、必要によって書き込み動作を行う装置が付随する場合もある。又、汎用のコンピュータを用いる場合は、各構成部は、一つのＣＰＵにソフトウエアという形で格納され、各出力端は、プリンタ、モニター、その他表示装置、各入力端は、キーボード、マウス、イメージスキャナー、その他入力装置との直接又は間接的な接続が好適にされる。

【００１２】次に図３を用いたより具体的な他の実施例について説明する。図３中②～⑧は、下記の符号②～⑧と一致するものであり、その各構成における詳細な動作の説明は上述に従うものとしてその説明は省略した。

①　ユーザー（１２）はInternet上（１０）のショップ（１１）のHomepage上で商品を選び、クレジットカード番号VCCによる決済を選ぶ。

②　ユーザー（１２）・ショップ（１１）間で暗号通信

と相手認証を行った後、ユーザー（１２）はショップ（１１）にカード番号、商品金額等を秘密鍵を用いて暗号化して送る。ユーザー（１２）はショップ（１１）と通信する公開鍵を持っていなければCA（１４）に問い合わせ公開鍵をもらう。認証の際は、例えばある特定のメッセージを相手が復号できるように暗号化して相手に送る。相手が無事復号化できたら正式な相手と認証できるメッセージ認証方式、ある平文とこれを書き手しか暗号化できない一方向性関数で処理した暗号文をセットにして送る。受け手は暗号部分を復号化し、平文と同じ内容であることを確認して初めて書き手が書いたものであると判断でき、署名の役割を果たすデイジタル署名方式等を用いることができる。尚、ユーザ（１２）－ＰＧ（カード会社、クレジット管理機関等を含む）間、ショップ－ＰＧ間と間接的にユーザ（１２）－ショップ（１１）間を認証することも可能である。必ずしも認証を必要としない。また、ユーザ（１２）－ショップ（１１）間の認証に関わらず、ショップ（１１）にカード番号を教えない場合は、ユーザ（１２）は、ショップ（１１）の公開鍵ではなく、ＰＧ（１３）の公開鍵で暗号化してショップ（１１）へ送ることとなる。この時ユーザ（１２）は、ＰＧ（１３）と通信する鍵を持っていなければＣＡ（１４）に問い合わせ鍵をもらうことになる。

❸ ショップ（１１）はそのクレジットカード番号VCCが登録されているPG（１４）へ問い合わせをする。この時、ショップ（１１）－PG（１４）間で相手認証、暗号通信をも行う。ショップ（１１）はPG（１４）と通信する公開鍵を持っていなければCA（１３）に問い合わせ公開鍵をもらう。

❹ PG（１４）はユーザー（１２）に対して認証を要求する。この時ユーザー（１２）・ショップ（１１）間は相手認証、暗号通信をも行う。ユーザー（１２）とPG（１４）はお互いに相手と通信する公開鍵を持っていなければCA（１３）に問い合わせ公開鍵をもらう。

❺ ユーザー（１２）とPG（１４）はお互いに相手認証を行う。

❻ PG（１４）はショップ（１１）に対してユーザー（１２）の認証結果とユーザー（１２）の与信結果を渡す。

❼ ショップ（１１）はPG（１４）に売り上げ処理を依頼する。

❽ ショップ（１１）はユーザー（１２）に購入のOK/NGの結果を返す。

【００１３】暗号方式としてＫＰＳ（Key Predistribution System）方式を用いた場合の本発明の他の実施例について図４、図５を参照して詳細に説明する。ＫＰＳ方式とは、相手の識別子を自分の秘密アルゴリズムに施して相手と共通鍵を作成する方式である。秘密アルゴリズムの作成等の作業は主にセンターに於て行われ、独自にセンタアルゴリズムを所持し、このセンタアルゴリズムにユーザ等の識別子を施して、各々固有に所持される秘密アルゴリズムを作成する。センタアルゴリズムの作成方法、秘密アルゴリズムの作成方法、及び共有する暗号鍵の作成方法、識別子の定義等、共有鍵を作成するまでの行程に係わる方法及び内容は、特開昭６３－３６６３４号、特開昭６３－１０７６６７号公報等に示されており、本発明は、これを好適に利用する。秘密アルゴリズムとしては（Blom,R.,"Non-Public Key Distribution," Advances in Criptology:Proceedings of CRYPTO'82,Plenum Press,1982,231-236）に示されるアルゴリズムも場合によっては適用可能である。

【００１４】図４を参照し、ユーザー（１２）のＫＰＳ加入登録時の動作について説明する。図中❶～❹は、下記の符号❶～❹と一致するものである。

❶ ユーザー（１２）は通常のクレジットカードと同様にカード会社PG（１４）へ申し込む。

❷ これも通常のクレジットカードと同様にカード会社PG（１４）が本人調査を行い、ＯＫであれば鍵発行機関に秘密アルゴリズムの発行を依頼する。NGであればここで終わりとなる。

❸ KPSセンタ(KPS鍵発行センタ)（認証機関CA（１３））が秘密アルゴリズムを生成し、カード会社PG（１４）へ送る。認証機関CA（１３）は、暗号方式としてＫＰＳシステムを用いる場合、センタアルゴリズムを所有し、ＫＰＳ加入者等に対し、加入者の識別子をこのセンタアルゴリズムに施して、加入者固有の秘密アルゴリズムを作成し、出力する機能を有する他、その機能に基づく加入者のデータを管理し、要請に応じ、認証機能を併せて有する場合もある。

❹ カード会社PG（１４）はユーザー（１２）へクレジットカード番号と秘密アルゴリズムをセットで秘密な状態で送る。秘密な状態であればいかなる手法でもよい。

【００１５】使用時の具体的な構成を図５（ａ）に示した。図５（ａ）において、（１１）は、商品、サービス等を提供する販売部であり、（１２）は、ユーザーであり、（１４）は、クレジット機関部である。各構成は上述した通りである。それぞれ、図示はしないが、通信回線を使用可能な端末を備え、何れの部も端末を介して通信を行う状態を備えている。（１１１），（２１１），（４１１）は、秘密アルゴリズム実行手段であり、それぞれが、秘密アルゴリズムを秘密に保持しこれを実行し、共有鍵を出力する手段であって、　その作成は、例えば、販売部（１１）は、認証機関CA（１３）に自分の識別子ID1を送付し、認証機関CA（１３）は、秘密に所有するセンタアルゴリズムにこの識別子ID1を施して秘密アルゴリズムを作成してこれを販売部（１１）に送付して得られるものである。具体的作成方法は上述したＫＰＳ関連公知文献に記載されている方法等を好適に利用するものである。秘密アルゴリズム実行手段（２１１）は、ユーザー（１２）が、認証機関CA（１３）に自分の

識別子ID2を送付して得られたものであり、秘密アルゴリズム実行手段（４１１）は、カード会社PG（１４）が認証機関CA（１３）に自分の識別子ID4を送付して得られたものである。図中、各秘密アルゴリズム実行手段は、２つの入力をそれぞれ示しているが（例えば図５（ａ）において、秘密アルゴリズム実行手段（１１１）に対し、ID2,ID3を入力する入力部が示されている。）、２つの入力部を有する構成を要するのではなく、１つの入力部に対し、逐次入力するものであってもよい。（１１２），（２１２），（４１２）は変換器であり、暗号化アルゴリズム、復号化アルゴリズムを有し、且つこれを実行するものである。この暗号化、復号化アルゴリズムは、例えば、ＤＥＳ、ＦＥＡＬ等の暗号アルゴリズムの他、鍵を用いるアルゴリズムであれば、如何なるアルゴリズムであってもよい。(1A)(2A)(4A)は、入力部であり、キーボード、テンキー、スキャナー等のデータを手動にて入力する機器、或は目的に応じて自動的にデータを出力する手段と直接的または間接的に接続する。(1B),(2B),(4B)は、主に復号されたデータを出力する部分であって、デイスプレイ、プリンタと直接的、間接的に接続し、或は、データ処理部と接続されるものである。H(1A)、H(2A)、H(4A)は、暗号化したデータを出力する部分であり、Ｉ(1)、Ｉ(2)、Ｉ(4)は、通信回線を介してデータを入力する部分である。図５（ａ）は、認証機関CA（１３）より秘密アルゴリズムがそれぞれに配布された後、クレジット番号等のクレジットデータによる取引を行う際の動作について説明する為の図である。

【００１６】・ユーザー（１２）は、複数の販売部の何れかの販売部（１１）を指定した後、購入しようとする商品或いは提供を受けようとするサービスを指定する。
・販売部（１１）は、利用可能なクレジット機関部をユーザー（１２）に伝達示唆する。
・ユーザー（１２）は、自分の利用可能なクレジット機関部（１４）を指示する。
この状態において、それぞれ相手の識別子(ID1,ID2,ID4)を入手済みとする。尚、識別子の場合、電話番号、住所、生年月日等、通常一般性の高い符号が用いられることから、公開鍵のような、認証機関からの供与を得る必要は全くなく、通信相手、商品カタログ、雑誌、その他公の機関等から自由な形で得られるものである。

【００１７】ユーザー（１２）は、販売部（１１）の識別子ID1とクレジット機関部（１４）の識別子ID4を自分の秘密アルゴリズム実行手段（２１１）に入力し、共有鍵K12、K24を出力する。販売部（１１）は、ユーザー（１２）の識別子ID2とクレジット機関部（１４）の識別子ID4を自分の秘密アルゴリズム実行手段（１１１）に入力し、共有鍵K12、K14を出力する。クレジット機関部（１４）は、販売部（１１）の識別子ID1とユーザー（１２）の識別子ID2を自分の秘密アルゴリズム実行手段（４１１）に入力し、共有鍵K14、K24を出力する。この共有鍵に基づき、それぞれ認証データの暗号化通信を行い、認証を行う。認証は、上述した様に相手との共有鍵を生成し、この共有鍵を変換手段に入力した状態で、認証データの交換を行うことによって行われる。

【００１８】ユーザー（１２）は、この共有鍵K12を暗号化器（２１２）に入力した状態でクレジット番号を入力部（2A）より入力する。暗号化器（２１２）は、入力されたクレジット番号を暗号化して販売部（１１）へ送る。販売部（１１）は、この暗号化データを入力部Ｉ(1)を介して入力し、共有鍵K12に基づいて、変換器（１１２）により復号化してそのクレジット番号を確認し、その旨を、クレジット機関部（１４）に送付する。送付の際、クレジット機関部（１４）の識別子ID4を自分の秘密アルゴリズム実行手段（１１１）に入力して、共有鍵K14を作成し、変換器（１１２）の入力部（1A）にクレジット番号及びその他の情報を併せた情報を入力してこれを暗号化（Ｈ(1A)）し、クレジット機関部（１４）に出力する。クレジット機関部（１４）は、販売部（１２）の識別子ID1を自分の秘密アルゴリズムに入力して、共有鍵K14を作成し、これを変換手段（４１２）に入力し、更に販売部から送られてきたH(1A)を入力部Ｉ(4)を介して変換手段（４１２）に入力してユーザー（１２）のクレジット番号を復号して入手し、照合、検索を行ってその結果データを販売部（１１）へ送付する。この送付は、相手識別子を秘密アルゴリズム実行手段（４１１）に入力した結果得られる共有鍵K14に基づき上述の記載のような動作で行われる。販売部（１１）は、クレジット機関部（１４）から送られてきたデータに基づき販売等の取引を行うものである。この際、取引停止等の意志表示をする際、上述の様に相手の識別子を、自分の秘密アルゴリズムに施して得られる共有鍵に基づいた暗号による通信を行ってもよい。

【００１９】図５（ｂ）を参照して、ＫＰＳ方式による商取引の際の動作の説明を行う。図中②～⑧は、下記の符号②～⑧と一致するものであり、その各構成における詳細な動作の説明は上述に従うものとしてその説明は省略した。
①ユーザー（１２）はInternet（１０）上のショップ（１１）のHomepage上で商品を選び、クレジットカード番号VCCによる決済を選ぶ。
②ユーザー（１２）・ショップ（１１）間で暗号通信と相手認証を行った後、ユーザー（１２）はショップ（１１）にカード番号、商品金額等を暗号化して送る。尚、ユーザ（１２）－ＰＧ（カード会社、クレジット管理機関等を含む）間、ショップ－ＰＧ間と間接的にユーザ（１２）－ショップ（１１）間を認証することも可能である。必ずしも認証を必要としない。また、ユーザ（１２）－ショップ（１１）間の認証に関わらず、ショップ（１１）にカード番号を教えない場合は、ユーザ（１

2）は、ショップ（１１）の公開鍵ではなく、ユーザ（１２）－ＰＧ（１３）間の共通鍵で暗号化してショップ（１１）へ送ることとなる。

❸ショップ（１１）はそのクレジットカード番号VCCが登録されているPG（１４）へ問い合わせをする。この時、ショップ（１１）－PG（１４）間で相手認証、暗号通信をも行う。

❹ PG（１４）はユーザー（１２）に対して認証を要求する。この時ユーザー（１２）・ショップ（１１）間で相手認証、暗号通信をも行う。

❺ ユーザー（１２）とPG（１４）はお互いに相手認証を行う。

❻ PG（１４）はショップ（１１）に対してユーザー（１２）の認証結果とユーザー（１２）の与信結果を渡す。

❼ ショップ（１１）はPG（１４）に売り上げ処理を依頼する。

❽ ショップ（１１）はユーザー（１２）に購入のOK/NGの結果を返す。

【００２０】ＫＰＳ方式を用いた場合、グループ内の２つの部間は、その他の部間と、暗号化内容が全く異なる為、異なる空間で通信が行われるのと同等となることから、各部から区別したデータを逐次送信する必要がなく、１つの部は、暗号化クレジット番号データとその他の同時送信可能なデータをまとめた形で送ってもよいことから、通信操作が極めて簡易になる。　例えば、図５のような構成を用いて図６で示すような１画面による操作により送付先全てに必要なデータを同報的に送付することも可能である。図６は、本発明の他の実施例を示したものである。最初、購入希望対象に応じて、販売部を指定する。販売部は、取扱可能なクレジット機関を指定し、表示する。購入の意志表示の前後において、購入モードを指定する。各送付先、即ち販売部（１１）、クレジット機関部（１４）のエリアに認証用データを入力し、クレジット番号を入力し、送信をクリック等して操作する。この際、ショップとの認証データの入力欄（１２Ｂ）、ＰＧとの認証データの入力欄（１２Ｃ）及びクレジット番号入力欄（１２Ａ）にそれぞれ、数値、データを入力し、同画面左欄に各々の識別子に相当するＩＤを入力する。販売部先データは、図５（ｂ）で示す販売部識別子ID1を秘密アルゴリズム実行手段に入力して得られる共有鍵K12で暗号化し、クレジット機関部へのデータは、図５（ｂ）で示すクレジット機関部の識別子ID4を秘密アルゴリズム実行手段に入力して得られる共有鍵K14で暗号化し、これら複数の暗号データを連結させて複数の宛先へこの連結した１組のデータを同報的に送付する。送付された側は、単に余分なデータを受信するだけで、その分は暗号化されているので、受信側に知られることはなく、なんら通信の安定性を損なうものではない。従って、この様に一度に複数のデータを送ることができるので、通信手続きを簡素化可能であり、利用者にとって手間のかからない取引を実現することができる。尚、暗号方式としてＫＰＳ方式を採用した場合を上記に示したが、公開鍵方式の場合であっても、秘密鍵及びこれに対応する公開鍵を複数登録しておくなどして、送付先ごとにその使用を変更すれば、適用可能である。尚、上記実施例においては、クレジット番号等、そのグループに一時的、継続的に加入することにより得られる記号、番号、符号等を暗号化した状態で伝達する場合を主に示すものであるが、他方クレジット番号を直接伝送するのではなく、、このクレジット番号に対応した会員番号等の他の番号で代用することで、クレジット番号の通信路からの漏洩を防ぐこともできる等安全性を向上させることができるものである。又、本人認証の際、パスワード等の本人固有で当事者以外には秘密の情報を不可したものであってもよい。更に本発明では、注文書等の取引上必要となる情報をショップ、ＰＧ等の認証機関向けに送信する場合、各個別に別々の鍵で暗号化或いはデジタル署名をし、必要とされる情報をすべて暗号に変換した後、同報的な通信を行い送付してもよい。この場合は、一度に手続きを終了させることができ、利便性が高い。又、ショップからユーザ、認証機関、クレジット会社等へ出力される領収書等も同様に、同報的に送るものであってもよい。この様に同報性を有する通信の場合の個別の暗号化は、暗号鍵が用事複数でも、単数でも秘密に容易に作成されることから暗号鍵の管理が不要なＫＰＳ方式が好適に用いられるものである。

【００２１】

【発明の効果】以上詳述のごとく本発明は、インターネット等の通信回線上で、クレジットカードを要しない仮想的なカードを使用し且つカード情報等を一旦暗号等の変換処理を施して通信することにより、取引認証など、買物とは別の手続きを少なくでき、合理的且つ安全に商取引ができる等の効果を有する。

【図面の簡単な説明】

【図１】本発明の一構成例を示す図。

【図２】

【図３】本発明の一実施例を示す図。

【図４】

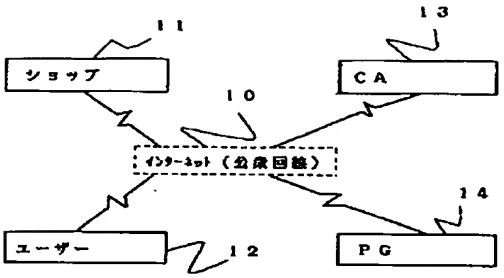
【図５】本発明の他の実施例を示す図。

【図６】本発明の他の実施例を示す図。

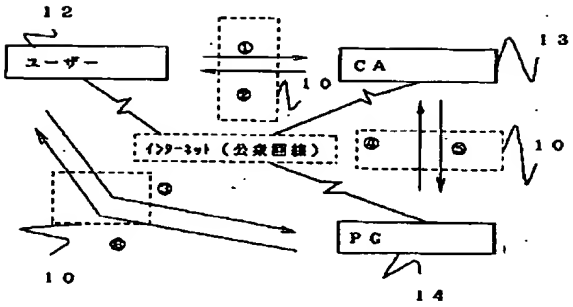
【符号の説明】

１０　通信回線
１１　ショップ
１２　ユーザー
１３　認証機関
１４　クレジット管理機関

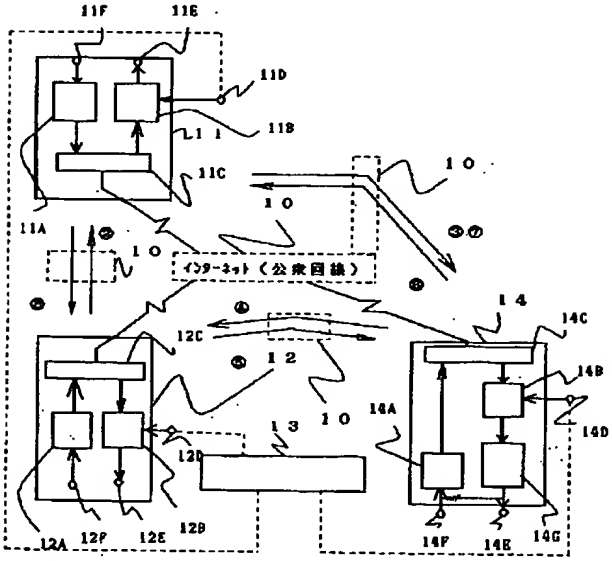
【図1】


11
13
ショップ
CA
10
インターネット（公衆回線）
14
ユーザー
12
PG

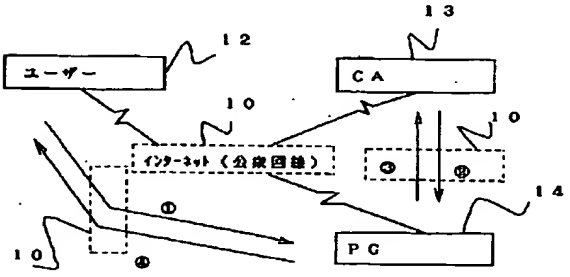
【図2】


12
ユーザー
①
②
10
CA
13
インターネット（公衆回線）
④
⑤
10
③
⑥
PG
10
14

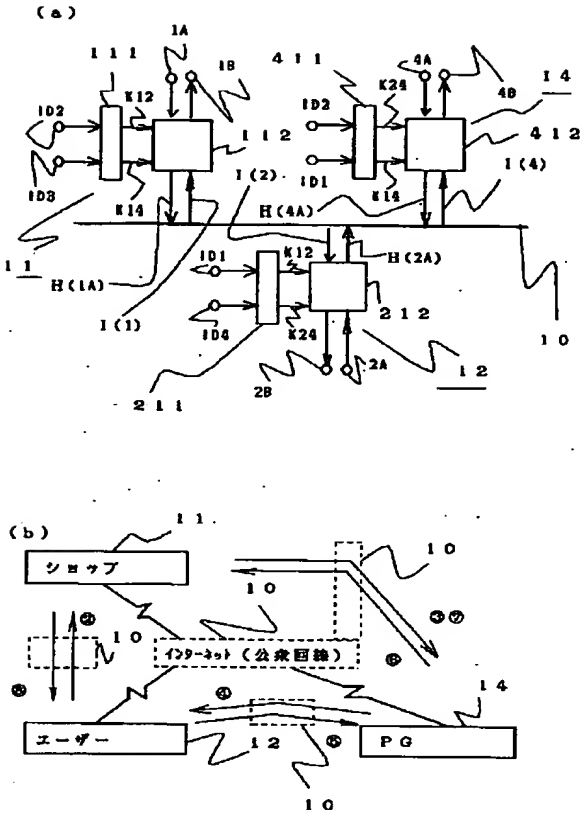
【図3】


11F
11E
11D
11B
L11
11C
10
11A
インターネット（公衆回線）
14
14C
12C
12
14B
10
14A
13
14D
12D
12A
12F
12E
12B
14F
14E
14G

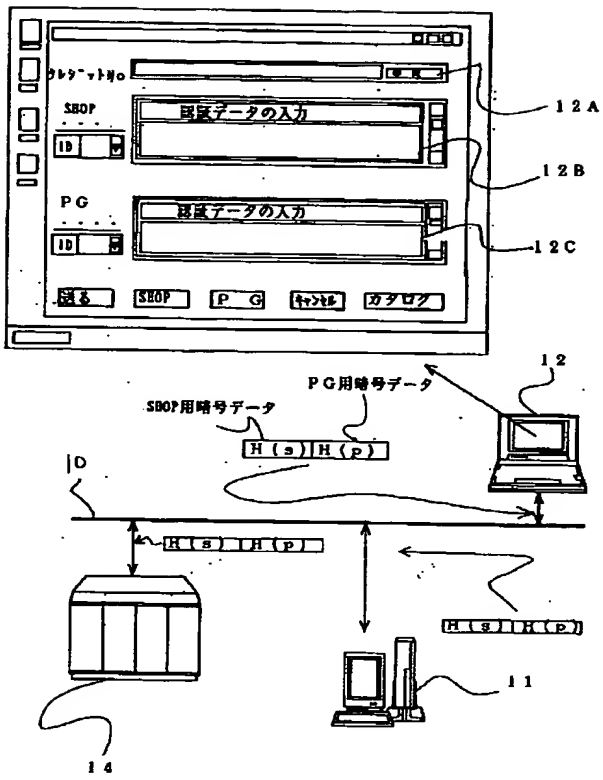
【図4】


13
12
ユーザー
CA
10
10
インターネット（公衆回線）
③
④
14
①
PG
10
②

【図5】


(a)
1A
111
1B
411
4A
4B
14
ID2
K12
K24
112
412
ID3
I(2)
ID1
I(4)
K14
K16
H(4A)
11
H(1A)
ID1
K12
H(2A)
I(1)
ID4
K24
212
10
2A
12
2B
211
(b)
11
ショップ
10
10
インターネット（公衆回線）
14
ユーザー
12
PG
10

【図6】


SHOP
認証データの入力
ID
PG
認証データの入力
ID
戻る
SHOP
P G
キャンセル
カタログ
12A
12B
12C
12
PG用暗号データ
SHOP用暗号データ
H(s)H(p)
ID
H(s)H(p)
H(s)H(p)
11
14